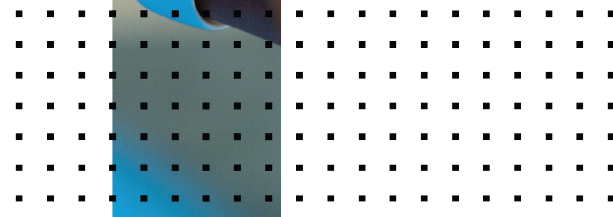
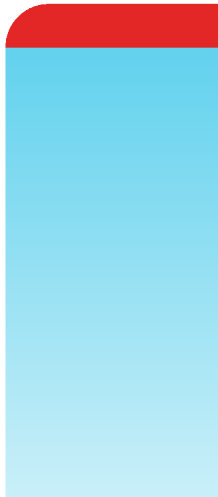


Release Notes

IPS Engine 7.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 09, 2022

IPS Engine 7.1 Release Notes

43-700-805146-20220509

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new in IPS Engine 7.1 build 124	6
Product integration and support	7
Resolved issues	8
Known issues	10

Change log

Date	Change Description
2022-05-09	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 7.1 build 124.

- [What's new in IPS Engine 7.1 build 124 on page 6](#)
- [Product integration and support on page 7](#)
- [Resolved issues on page 8](#)
- [Known issues on page 10](#)

IPS Engine 7.1 build 124 is a release to FortiGuard for FortiOS 7.0. It is not a built-in release for FortiOS.

For additional FortiOS documentation, see the [Fortinet Document Library](#).

What's new in IPS Engine 7.1 build 124

Bug ID	Description
728408	Support for expect sessions in next generation firewall policy mode.

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	7.0
---------	-----

Resolved issues

The resolved issues listed do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
644638	Policy with Tor-Exite.Node as source does not block traffic coming from TOR.
683066	IPS engine crashes and consumes high CPU.
698247	IPS Engine has several signal 6 crashes at <code>ovrd_svr_write_done</code> on corporate firewall.
713508	Download performance is low when SSL deep inspection is enabled.
718503	IPS Engine uses high memory usage.
730235	FortiGate 5001E/5001E1 image build0202 7.0.2 IPS Engine application crashes during traffic testing.
752466	Deep inspection causes downloads to fail in autodiscovery VPN environment.
752540	FortiGate outputs warning messages while rebooting.
754216	Flow mode web filter replacement message does not display using upstream proxy when HTTPS.
754579	Application performance is ten times worse when IPS Engine is applied in flow mode.
755223	There is no detection trigger packet in PCAP.
755294	Deep inspection is very slow and certificate errors occur in proxy or flow mode.
755851	Mixed mode inspection causes SSL error for passthrough proxy traffic.
756398	An invalid character string is inserted in the IPS Engine log sent to the TCP SYSLOG server.
756616	High CPU in proxy-based policy with deep inspection and IPS sensor.
757122	Wildcard string does not work as described in the Administration Guide.
757314	IPS Engine crashes after upgrade and affects traffic.
757951	IPS Engine cannot block Common Internet File System oversize files.
759194	FortiGate inserts wrong timestamp into PCAP data.
760555	Web Filter Unified Threat Management logs unexpected URL such as <code>url=https:///""</code> .
765859	Repeated IPS Engine signal 11 and signal 7 crashes.
770685	Traffic does not match the security policy with SD-WAN zone (PPPoE interface) in next generation firewall (NGFW) mode.
774826	IPS Engine processes consume high CPU usage.
774957	Web Filter URL static filter blocks all traffic.

Bug ID	Description
775566	Some websites do not load in flow-based mode with deep SSL inspection.
777464	Update crashes after running scripts.
781894	Website does not open based on the matching policy when using Web Filter in NGFW mode.
781898	User cannot upgrade FortiGate from 7.0.3 to 7.0.4 or 7.0.5.
790490	Shared memory is not released and causes the device enter conserve mode.
792312	HTTPS traffic cannot pass VMware ESXi FortiGate-VM well when IPS Engine and deep inspection are enabled.
802465	ERR_SSL_PROTOCOL_ERROR occurs when loading a website in flow mode.

Known issues

There are no known issues with this release of IPS engine version 7.1 for FortiOS.

To report a bug, please contact [Customer Service & Support](#).



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.